署名偽造攻撃の次世代電子パスポートへの適用

酒見 由美† 伊豆 哲也‡ 武仲 正彦‡ 野上 保之† 森川 良孝†

† 岡山大学
〒 700-8530 岡山市北区津島中 3-1-1
{sakemi,nogami,morikawa}@trans.cne.okayama-u.ac.jp

‡ 株式会社富士通研究所
〒 211-8588 川崎市中原区上小田中 4-1-1
{izu,takenaka}@labs.fujitsu.com

あらまし 出入国の厳格かつ迅速な管理を目的として, 国際民間航空機関 (ICAO) は電子パスポート (e-Passport) の導入を推進しており, 日本を含むいくつかの国で既に発行が開始されている. 2009 年 8 月に開催された国際会議において Coron, Naccache, Tibouchi, Weinmann は次世代の e-Passport が使用する ISO/IEC 9796-2 署名の偽造攻撃法と, 実際の偽造署名データを発表した. 本稿は Coron 等の署名偽造攻撃を次世代 e-Passport に適用した場合の偽造可能性を議論する.

Applying the Forgery Attack to the Next-generation e-Passport

Yumi Sakemi† Tetsuya Izu‡ Masahiko Takenaka‡ Yasuyuki Nogami† Yoshitaka Morikawa†

†Okayama University,
3-1-1, Tsushima-naka, Kita-ku, Okayama,
700-8530, Japan
{sakemi,nogami,morikawa}@trans.cne.okayama-u.ac.jp

‡FUJITSU Lab.,
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki,
211-8588, Japan
{izu,takenaka}@labs.fujitsu.com

Abstract For establishing strict and rapid immigration control, ICAO has been spreading the electronic passport (e-Passport), which is introduced in some countries including Japan. Very recently, on August 2009, Coron, Naccache, Tibouchi, and Weinmann announced a new forgery attack against the signature scheme ISO/IEC 9796-2, which will be used in the next-generation e-Passport. This paper discusses the possibility and the effect when the attack is applied to the next-generation e-Passport.

1 はじめに

出入国における厳格かつ迅速な管理を目的として, ICAO (国際民間航空機関; International Civil Aviation Organization) は電子パスポート (e-Passport) の標準化を積極的に推進している [ICAO]. 2004 年 10 月に公開された e-Passport の最初の仕様では, 電子データ (MRTD; Machine Readable Travel Documents) の完全性保護機能 (PA; Passive Authentication) と基本的なアクセス制御機能 (BAC; Basic Access Control) が搭載され, いくつかの国で既に導入されている (日本では 2006 年 3 月に e-Passport の発行が開始された). さらにクローニング防止機能 (AA; Active Authentication) を実現する次世代 e-Passport の仕様策定も進んでおり, ISO/IEC 9796-2 Scheme

1 (以下, 単に ISO/IEC 9796-2 署名と記す) と呼ばれる素因数分解問題 (RSA) をベースとした署名方式が使用される予定となっている [IPA09].

一方で, 2009 年 8 月に開催された暗号国際会議 CRYPTO 2009 において, Coron-Naccache-Tibouchi-Weinmann は ISO/ IEC 9796-2 署名の偽造攻撃 (CNTW 攻撃) を発表し [CNTW09], 2048-bit 合成数を用いた ISO/IEC 9796-2 署名の計算機による偽造が約 2 日で可能であることを報告した. しかし特定の条件下での攻撃コストしか評価されていないため, 他の条件下での CNTW 攻撃の脅威が判断しにくいという問題があった.

本稿の目的は, CNTW 攻撃の詳細評価を与えることと, CNTW 攻撃を次世代 e-Passport に適用した場合の偽造可能性を議論することである. 結果として, 確かに次世代 e-Passport は ISO/IEC 9796-2 署名を用いているものの, CNTW 攻撃を適用しても偽造署名を算出できる可能性は極めて低いという結論を得た. しかし e-Passport の有効期限が比較的長期 (日本は最長 10 年) であり, 攻撃が改良される可能性がある以上, 次世代 e-Passport における ISO/IEC 9796-2 署名の使用は避けるべきである.

2 ISO/IEC 9796-2 署名について

本節では, ISO/IEC 9796-2 署名 [ISO] のアルゴリズムと, 2009 年 8 月に提案された Coron-Naccache-Tibouchi-Weinmann による署名偽造攻撃 (CNTW 攻撃) [CNTW09] を説明する.

2.1 ISO/IEC 9796-2 署名

ISO/IEC 9796 ではメッセージの部分 (または完全) 復元が可能な署名方式が規定され, 素因数分解問題 (RSA) を利用した方式 ISO/IEC 9796-2 [ISO] と, 離散対数問題を利用した方式 ISO/IEC 9796-3 とに分かれている. 2002 年に制定された現行の ISO/IEC 9796-2 では 3 つの方式 (Scheme 1, 2, 3) が記述されている. 本稿の考察対象は Scheme 1 であるため, 以下では Scheme 1 を単に ISO/IEC 9796-2 署名と記す.

セキュリティパラメータ k に対し, $(\mathsf{sk}, \mathsf{pk})$ を署名者の秘密鍵・公開鍵ペアとする. ただし $\mathsf{sk} = (p, q, d)$, $\mathsf{pk} = (N, e)$, p, q は $k/2$-bit 素数, $N = p \times q$ は k-bit 合成数, d, e は $de \equiv 1 \pmod{(p-1)(q-1)}$ を満たす整数とする. このときメッセージ m に対する署名は $\sigma = \mu(m)^d \bmod N$ によって与えられる. ここでパディング関数 $\mu(\cdot)$ は

$$\mu(m) = \texttt{0x6A}||m[1]||H(m)||\texttt{0xBC} \qquad (1)$$

と定められており, $H(\cdot)$ は出力長 k_H (≥ 160) bit のハッシュ関数, $m[1]$ はメッセージ m の上位 $(k - k_H - 16)$-bit を示す. 0x6A はパディングが ISO/IEC 9796-2 (部分復元) であることを示すヘッダ, 0xBC はハッシュ関数が SHA-1 であることを示すトレーラである. 署名 σ を受け取った検証者は, $\overline{m} = \sigma^e \bmod N$ によってパディングされたメッセージ $\overline{m}$ を構成し, フォーマットを満たしているかをチェックする.

2.2 CNTW 攻撃

2009 年 8 月に開催された国際会議 CRYPTO 2009 において, Coron, Naccache, Tibouchi, Weinmann は, ISO/IEC 9796-2 署名の新しい偽造方法 (CNTW 攻撃) を提案し, 実際に偽造が可能であることを計算機実験によって確認した [CNTW09].

CNTW 攻撃 (およびベースとなった攻撃) の目標は, 偽造メッセージを m^* とするとき, L 個のメッセージ $m_1, m_2, \ldots, m_L$ による積表現 $\mu(m^*) = \delta^e \mu(m_1)^{e_1} \mu(m_2)^{e_2} \cdots \mu(m_L)^{e_L} \bmod N$ を導出することである (δ は係数, $1 \leq e_1, e_2, \ldots, e_L < e$). このとき, それぞれのメッセージに対応する署名間の積表現は

$$\sigma^* = \sigma_1^{e_1} \sigma_2^{e_2} \cdots \sigma_L^{e_L} \bmod N \qquad (2)$$

となるため, 攻撃者が $\sigma_1, \sigma_2, \ldots, \sigma_L$ を入手できれば, 偽造署名 σ^* を実際に導出できる.

上のようなメッセージ間の積表現を算出するために, Desmedt-Odlyzko は $\mu(m_i)$ の素因数分解を利用した方法を提案した [DO85] が, 実際に署名を偽造するには, $\mu(m_i)$ は 200-bit 以下でなければならず, ISO/IEC 9796-2 には適用できなかった. そこで Coron-Naccache-Stern は $\mu(\cdot)$ の代わりに, $\mu(\cdot)$ から算出される関数

$$\nu_{a,b}(\cdot) = a \cdot \mu(\cdot) - b \cdot N \qquad (3)$$

の素因数分解を利用した方法を提案した (CNS 攻撃) [CNS99]. パラメータ a, b を適切に設定する

ことで $\nu_{a,b}(\cdot)$ は高々 (k_H+16)-bit となるため, 偽造に必要な計算量は $k_H=128$ のときで 2^{54}, $k_H=160$ のときで 2^{61} に削減される. しかし ISO/IEC 9796-2 署名の実際の偽造には至っておらず, 理論的な偽造可能性を示すに留まっていた.

Coron-Naccache-Tibouchi-Weinmann はパラメータ a, b を最適化し, 出力値が高々 $(k_H+|a|)$-bit になることを示した. また Coron-Naccache-Stern アルゴリズムの各処理の実装を高速化し, (実質的に) $(k_H+|a|-8)$-bit 以下となるメッセージだけを扱うことで, 署名に関する積表現の算出に成功した [CNTW09]. 具体的には, N が 2048-bit の合成数, $e=2$, ハッシュ関数が SHA-1, $|a|=10$ の場合に (このとき $\nu_{a,b}(m)$ が実質的に 162-bit 以下となるようなメッセージ m だけを扱っている), 約 2 日間で偽造署名が算出できることを示した. 計算環境には Amazon のクラウドコンピューティングサービス EC2 を利用し, 約 800 ドル分の計算リソースを使用した.

2.3 CNTW 攻撃の影響

CNTW 攻撃は積表現 (2) を用いて偽造署名を導出するため, 攻撃者は L 個の正当な署名を必要とする. しかしハッシュ関数として SHA-1 を用いた場合, L は膨大 (上の実験では $L=2^{18.7}$) であり, これら署名の入手は現実的には困難である. また攻撃者が署名を入手して偽造署名 σ^* を導出できたとしても, 対応する偽造メッセージ m^* の上位 $(k-k_H-16)$-bit は偽造過程で自動的に定められるため, m^* の上位ビットはほぼランダムとなり, 意味のあるデータとなる可能性は低い.

以上のことから, CNTW 攻撃は ISO/ IEC 9796-2 署名の偽造署名を算出できているものの, 現実社会における影響は無視できるほどに小さく, 何らかのシステムが ISO/IEC 9796-2 署名を使用しているからといって直ちに別の署名方式に移行する必要性は薄いと考えられる. しかし攻撃アルゴリズムのさらなる改良を加味すれば, これから新たに構築するシステムでは, ISO/IEC 9796-2 署名 (Scheme 1) の使用は避けるべきである (実際, Scheme 1 は既存システムとの互換性維持を目的とされており, 新システムでは Scheme 2, 3 の使用が推奨されている).

3 CNTW 攻撃の詳細評価

Coron-Naccache-Tibouchi-Weinmann は, 2.2 節で紹介した計算機実験のデータをもとに, 他の条件下での攻撃計算量を予想している [CNTW09]. しかし ISO/IEC 9796-2 署名においてハッシュ関数 SHA-2 を使用した場合にトレーラが 16-bit になること, また, 合成数 N を変化させたときのパラメータ a の振る舞いが考察されていないことから, 他の条件下での脅威が判断しにくいという問題がある. そこで本節では, CNTW 攻撃の詳細な計算量を算出・評価する.

3.1 CNTW 攻撃計算量の算出方法

CNTW 攻撃 (および, そのベースである CNS 攻撃) では, 署名に関する積表現 (2) を算出するために, パディング値が p_L-smooth となるようなメッセージ (とその素因数分解) を L 個以上収集する必要がある (ここで p_L は L 番目の素数であり, ある自然数が p_L-smooth であるとは, その自然数が p_L 以下の素数で素因数分解できることを指す). このメッセージ探索の計算量は署名偽造全体の計算量の大部分を占めるため, メッセージ探索の改良が必須となる. そこで CNTW 攻撃は, メッセージ探索を (1) p_L-smooth 判定テスト, (2) (p_L-smooth と判定された場合に) 素因数分解, の 2 段階に分割することでメッセージ探索を高速化した. 特に p_L-smooth 判定テストに Bernstein's smoothness detection algorithm (BSDA) を用いた場合, 試し割り算法に比べて約 1000 倍の高速化を実現した.

BSDA を用いた場合, n 個の s-bit の自然数が p_L-smooth であるかを判定するために必要な計算量は $O(t\cdot\log^2 t\cdot\log\log t)$ となる. ここで, t は n 個の s-bit 自然数のリストおよび p_L 以下の素数リストのサイズを表しており, $t=n\cdot s+L\cdot\log_2 L$ である [CNTW09]. ランダムな s-bit の自然数が p_L-smooth である確率を α とすると, パディング値が p_L-smooth であるメッセージを L 個収集するためには $n=L/\alpha$ 個のメッセージに対する smoothness 判定テスト (BSDA) が必要となる. CNTW 攻撃のように n が非常に大きくなる場合, $n'=n/k$ 個のメッセージに対する BSDA 処理を k 回行う方が効率が良い. 最適な n' を選択

した場合, メッセージ探索に必要な計算量は次式で与えられる:

$$C_{\mathrm{BSDA}} = n \cdot s \cdot t \cdot \log^2 t \cdot \log\log t \qquad (4)$$

さらに, CNTW 攻撃では Large Prime Variant と呼ばれるテクニックを利用して, BSDA の処理を施すメッセージの総数 n を削減している.

3.2 CNTW 攻撃のパディング関数

CNTW 攻撃が使用するパディング関数 $\nu_{a,b}(\cdot) = a \cdot \mu(\cdot) - b \cdot N$ の任意の入力値に対する出力値ができるだけ小さくなるような a, b の求め方を説明する. なお, ここではハッシュ関数に SHA-1 を用いる場合について述べる. $\mu(\cdot)$ と N がほぼ同じサイズであることと, $\mu(\cdot)$ の最上位及び最下位の各 8-bit が固定値であることから, a, b を適切に定めることで, $\nu_{a,b}(\cdot)$ の最上位, 最下位の各 8-bit を 0 にすることができる. さらにメッセージの上位 $(k - k_H - 16)$-bit の値 $m[1]$ を適切に定めることで, $\nu_{a,b}(\cdot)$ の上位 $9-(k-k_H-8)$-bit についても 0 にできる. その結果 $\nu_{a,b}(\cdot)$ の出力長を $(k_H + |a|)$-bit に削減した.

[CNTW09] では, 合成数 N として RSA2048 [RSA] を使用した場合に, 上の条件を満たす最小の a が 10-bit となることが報告されている. このとき BSDA の処理対象は 170-bit となる.

さらに CNTW 攻撃では, ハッシュ計算コストが, smoothness 判定テスト (BSDA) のコストに比べて十分に小さいことから, メッセージ m に対するパディング値 $\nu_{a,b}(m)$ の先頭 8-bit が 0 になるようなメッセージを選択している. これによって, BSDA の処理対象となるメッセージの大きさを実質的に $170 - 8 = 162$-bit に削減した.

3.3 パディング関数の詳細評価

[CNTW09] では, RSA2048 [RSA] に対する a, b だけしか議論されておらず, N を変化させた場合の a, b の振る舞いが不明である. そこで 2048-bit の RSA 型合成数を 5000 個準備し, SHA-1 を用いた場合の a の値とその分布を求めた (図 1). このとき a の平均値は 8.13-bit となり, ほぼ (8 ± 2)-bit 内に収まることが判明した.

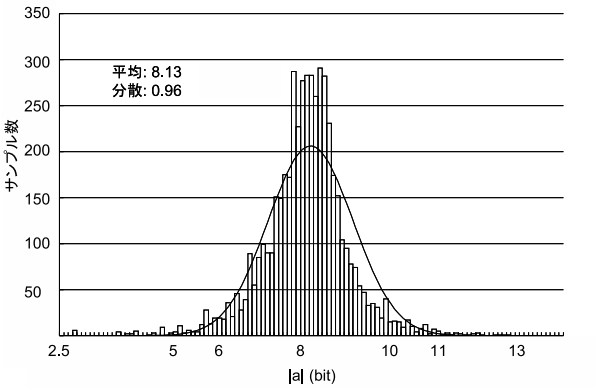

図 1: N が 2048-bit, SHA-1 使用時の a 値の分布

他方で [CNTW09] では, ハッシュ関数に SHA-256 を用いた場合でも, パディング関数 $\mu(\cdot)$ のトレーラを 8-bit として評価している. しかし SHA-256 を用いた場合, トレーラは 16-bit 値 0x34CC となるため, a, b の算出方法が変わってくる. 実際, SHA-256 を用いる場合, $\nu_{a,b}(\cdot)$ の最上位 8-bit と最下位 16-bit が 0 となるような, a, b を定めることが可能となる. SHA-1 の場合と同様に, N を変化させたときの a の分布を算出したところ, $|a|$ の平均値は 12 ± 2 となることが判明した.

同様に, ハッシュ関数に SHA-2 を用いた場合のトレーラは全て 16-bit となるため, パディング関数 $\nu_{a,b}(\cdot)$ の出力値は平均 $(k_H + 12)$-bit となることがわかる.

3.4 CNTW 攻撃の計算量評価

[CNTW09] では, 特定の合成数 (RSA2048) を用いた偽造実験の計算時間等の情報を用いて, 他の条件下での攻撃コストが評価されている. しかし 3.3 節で述べたように, a 値の分布やハッシュ関数の違いを考慮していないため, CNTW 攻撃の脅威が正確に判断できないという問題がある. そこで本節では, これらの差異を考慮した攻撃コストを算出する.

前節までの議論をふまえた攻撃コストの算出結果を表 1 に示す. ここで L は (4) の攻撃計算量が最小となる値, cost はその場合の攻撃計算量, τ は BSDA の処理を施す必要のあるメッセージ数である. また計算時間はシングルコア 2.4 GHz の PC 1 台を用いた場合であり, 積表現 (2) の算出に必要な時間である. 計算時間の評価には, Coron-Naccache-Tibouchi-Weinmann

表 1: 各ハッシュ関数に対する CNTW 攻撃の計算量

ハッシュ関数	$\lvert\nu_{a,b}(\cdot)\rvert$	$\log_2 L$	$\log_2$ cost	計算時間	$\log_2 \tau$	Amazon EC2 cost (US $)
SHA-1	160	21	55	0.5 年	38	454
SHA-224	228	27	67	1,286 年	48	1,110,777
SHA-256	260	29	72	34,874 年	52	30,131,119
SHA-384	388	38	88	3,902,163,409 年	68	3,371,469,185,653
SHA-512	516	46	103	84,083,141,453,024 年	81	72,647,834,215,413,100

表 2: SHA-1, SHA-256 の場合の計算コスト

SHA-1		SHA-256	
$\lvert\nu_{a,b}(m)\rvert$	$\log_2$ cost	$\lvert\nu_{a,b}(m)\rvert$	$\log_2$ cost
158	55.1	258	71.2
160	**55.5**	**260**	**71.5**
162	55.9	262	71.8

が算出した「ハッシュ関数が SHA-1 の場合にはシングルコア 2.4 GHz の PC 1 台で 1.8 年の計算時間が必要となる」という情報を用い, 各ハッシュ関数に対する cost の比から算出した. さらに Amazon EC2 cost は得られた計算時間から見積もった Amazon EC2 の使用料金である.

表 1 からわかる通り, ハッシュ関数として SHA-2 を使用する場合, SHA-224 の時点で署名偽造に約 1 億円分の計算リソースを必要とすることから, 本攻撃による署名偽造は難しいことがわかる.

また, SHA-1 および SHA-256 に対し 3.3 節で考察した a 値のゆらぎに対する攻撃計算量の違いを表 2 にまとめる. この表からわかる通り, 合成数 N によって, 攻撃計算量が約 20% 程度増減することがわかる.

4 次世代電子パスポートへの適用

本節では, ISO/IEC 9796-2 署名の利用が予定されている次世代の電子パスポートの概要と, CNTW 攻撃の適用可能性を検討する.

4.1 電子パスポート

2004 年 10 月に公開された電子パスポート (e-Passport) の最初の仕様では, 基本的なアクセス制御機能 (BAC) と電子データ (MRTD) の完全性保護機能 (PA) が規定された. 日本では, 2005 年 6 月に IC 旅券 (電子パスポート) の導入を定めた改正旅券法が公布され, 2006 年 3 月に発行が開始された. この仕様では, IC チップ内に保存された MRTD の改ざんと, IC チップとリーダ間の通信の盗聴は防止できるが, IC チップ内のデータの他の IC チップへのコピー (クローニング) は対策できていない. 実際, 電子パスポートデータをブランクカードへクローニングできることが報告されている [Gru06, Bee08].

これに対し, 次世代 e-Passport では, クローニング防止機能 (AA; Active Authentication) の導入が予定されてる. 日本でも次世代 IC 旅券に対するセキュリティ要件書 (PP; Protection Profile) が公開され [IPA09], 次世代 e-Passport 導入の準備が進められている.

4.2 CNTW 攻撃の適用検討

次世代 e-Passport のクローニング防止機能 AA は ISO/IEC 9796-2 署名を使用するため [IPA09], CNTW 攻撃の適用可能性が問題となる.

AA のプロトコルを図 2 に示す. AA では, まずパスポートリーダ (IFD; InterFace Device) が電子パスポート (ICC; IC Card) から AA 用の公開鍵を読み出す. IFD は, その公開鍵の正当性を PA により検証する. 次に IFD は 8-byte の乱数 $M2$ を生成し, ICC に送信する. ICC は 106-byte の乱数 $M1$ を生成し, メッセージ $M = M1||M2$ に対して, AA 用秘密鍵で ISO/IEC 9796-2 署名を生成し, IFD に返信する. 最後に IFD は, AA 用公開鍵を用いて署名を検証する.

ISO/IEC 9796-2 署名のメッセージエンコード処理を図 3 に示す [IPA09]. メッセージエンコードには 1024-bit 合成数と SHA-1 が使用されることとなっている. 本仕様では, ISO/IEC 9796-2

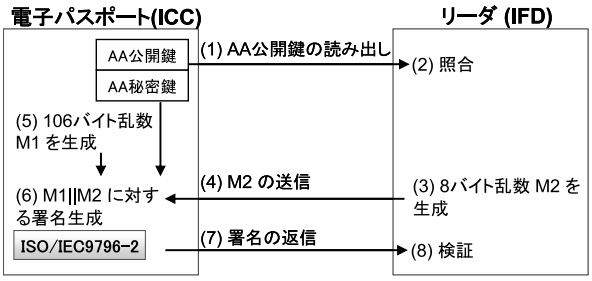

図 2: AA プロトコル

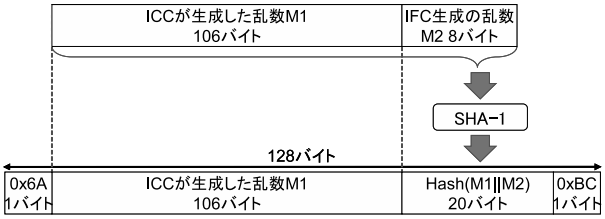

図 3: メッセージエンコード処理 [IPA09]

署名は, メッセージが部分的に復元されるモード (ヘッダが 0x6A) で使用され, 復元されるメッセージは ICC が生成した乱数 $M1$ となる. これにより, 乱数 $M1$ を署名と共に送信することなく, IFD による署名検証が可能となっている.

CNTW 攻撃では, 攻撃者はメッセージを自由に選択することが出来ないという限界があった (2.2 節). よって CNTW 攻撃を本仕様に適用した場合, 攻撃者はメッセージの復元される部分 ($M1$) を操作できず, メッセージのハッシュ値と重なる部分 ($M2$) しか変更できない. しかし AA では, 署名検証者である IFD が $M2$ を生成するため, 攻撃者による $M2$ の操作は意味を持たない. 以上の議論により, CNTW 攻撃を用いた AA の偽造は不可能であり, 次世代 e-Passport への現実的な影響は無視できるという結論を得る.

5 まとめ

本稿は, ISO/IEC 9796-2 署名に対する CNTW 攻撃を評価するとともに, 次世代 e-Passport のクローニング防止機能 AA への適用可能性を議論した. 結果として, CNTW 攻撃によって偽造署名を算出できる可能性は低く, 次世代 e-Passport に与える影響は極めて小さいという結論が得られた. しかし CNTW 攻撃が改良される可能性を加味すれば, 次世代 e-Passport における ISO/IEC 9796-2 署名の使用は避けるべきであろう.

他の観点から次世代 e-Passport の安全性を考えた場合, ISO/IEC 9796-2 署名の鍵長が 1024-bit である点と, ハッシュ関数 SHA-1 を使用する点は見直しが必要である. 具体的には, 鍵長を 2048-bit 以上とし, 出力長が 224-bit 以上のハッシュ関数を使用すべきである.

参考文献

[Bee08] J. Beek, “ePassports reloaded,” *Black Hat Japan 2008*.

[CNS99] J. Coron, D. Naccache, J. Stern, “On the Security of RSA Padding”, *CRYPTO 1999*, LNCS 1666, pp. 1-18, Springer-Verlag, 1999.

[CNTW09] J. Coron, D. Naccache, M. Tibouchi, R. Weinmann, “Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures”, *CRYPTO 2009*, LNCS 5677, pp. 428-444, Springer-Verlag, 2009.

[DO85] Y. Desmedt, A. Odlyzko, “A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes”, *CRYPTO 1985*, LNCS 218, pp. 516-522, Springer-Verlag, 1986.

[ICAO] “Machine Readable Travel Documents (Doc 9303) – Part 1: Machine Readable Passport – Volume 2: Specification for Electrically Enabled Passports with Biometric Identification Capability”, 6th edition, International Civil Aviation Organization (ICAO), 2006.

[IPA09] “IC 旅券用プロテクションプロファイル解説書”, 情報処理通信機構, 2009. Available at http://www.ipa.go.jp/security/fy20/reports/epassport/PP-guideVer1.0.pdf

[ISO] “Information Technology – Security Techniques – Digital Signature Schemes Giving Message Recovery – Part 2: Integer Factorization based Mechanisms”, International Organization for Standardization (ISO), 2002.

[Gru06] L. Grunwald, “Cloning ePassports without Active Authentication”, *BlackHat USA 2006*.

[RSA] RSA Laboratories, ”RSA numbers,” Available at http://en.wikipedia.org/wiki/RSA_numbers